

# Natural Security Version 5.1.1 Release Notes for UNIX and OpenVMS

These Release Notes describe the enhancements and new features that are provided with Version 5.1.1 of Natural Security for UNIX and OpenVMS.

In addition to providing the enhancements and new features described in these Release Notes, Natural Security Version 5.1.1 also consolidates all error corrections, modifications and enhancements provided with the previous patch-level releases of Natural Security. Version 5.1.1 contains all changes applied to Version 4.1.2 as error corrections.

This document covers the following topics:

- Using Multiple Versions of Natural Security
  - Central Administration in a Heterogeneous Environment
  - Administrator Services Enhancements
  - User Maintenance Enhancements
  - Library Maintenance Enhancements
  - Other Enhancements
- 

## Using Multiple Versions of Natural Security

The Natural Security system file FSEC can be shared by Natural Security Versions 4.1.1, 4.1.2 and 5.1.1.

To ensure the consistency and completeness of the security data on a shared FSEC file, it is strongly recommended that you use only the highest Natural Security version for Natural Security maintenance.

If you use a shared FSEC file, it is **not** necessary to transfer any security data with SECULD/ SECLOAD.

For further information, see the section Shared Natural Security System File FSEC under General Installation Information in the Natural Security installation documentation.

## Central Administration in a Heterogeneous Environment

With Natural Security, you can also control access to Natural in a heterogeneous environment, that is, an environment comprising Natural on a mainframe computer and Natural on various non-mainframe platforms (OpenVMS, UNIX, Windows NT/2000, and Windows 98).

To make security administration in such a heterogeneous environment easier, Natural Security Version 3.1 for mainframes allows you to store all security data in a single mainframe FSEC system file, and maintain them centrally for all other platforms in the heterogeneous environment using Natural Security on the mainframe computer.

Thus, security administration can be simplified and standardized on a company-wide basis.

The security data on the mainframe FSEC file are accessible from the non-mainframe platforms via Entire Net-Work. On a non-mainframe platform, you can retrieve these central security data, but not maintain them (neither directly nor via interface subprograms).

For further information on Natural Security in heterogeneous environments, please refer to your Natural Security documentation (Version 5.1.1 for OpenVMS, UNIX and Windows or Version 3.1 for Mainframes).

## Administrator Services Enhancements

### Administrator Services Menu/Set General Options/Logging of Maintenance Functions

This option displays a window in which you can determine the object types whose modifications are to be logged. In previous versions, "external objects" could only be marked collectively here, applying to all types of external objects; as of Version 5.1.1, you can activate/deactivate the logging for each type of external object individually.

### Administrator Services Menu 2/Processing of Maintenance Log Records

**List Log Records:** The Log File Maintenance batch-mode function "List Log Records" has been enhanced: In addition to listing the contents of the log file, it also displays for each record the components of the security profile concerned; moreover, the components that were modified will be marked. The batch report displayed corresponds to the information displayed by the function List Security Profile Maintenance Logs.

**External Objects:** Until Version 4.1.2, the object type "external objects" could only be selected collectively for the functions List Security Profile Maintenance Logs and Log File Maintenance. As of Version 5.1.1, you can select each type of external object individually.

## User Maintenance Enhancements

### Modify User/Time Differential Parameter

You can now set the Time Differential in user profiles of type TERMINAL not only to a value of hours/minutes, but also to "\*". This has the same effect as the Natural profile parameter TD=AUTO, which means that the time differential will be computed by comparison of physical and logical machine times.

### Modify User/Additional Options/Session Options/UNLOCK Parameter

For compatibility reasons, the Unlock parameter is now available under User/Additional Options/Session Options. However, the UNLOCK system command is not implemented on UNIX and OpenVMS systems.

## Library Maintenance Enhancements

### Additional Options/Restrictions/Session Parameters/DU Parameter

The DU parameter can now be set to ON/OFF/blank instead of T/F.

### Additional Options/Restrictions/Session Parameters - RPC Restrictions/Close All Databases

The new option Close All Databases allows you to control the logon/logoff-dependent closing of databases. It affects all databases which have been opened by remote subprograms contained in the library you are maintaining. The following settings are available:

N	The databases are not closed when a logon/logoff to/from the library is performed.
Y	The databases are closed when a logon to the library is performed.
F	The databases are closed when a logon to the library is performed, and when a logoff from the library is performed.

This option is only relevant if the option LOGONRQ=ON is set in the Natural profile parameter RPC or NTRPC macro. If you wish to have one user-queue element per client session for each database accessed by the RPC server, it is recommended that you set LOGONRQ=ON and "Close All Databases" to "Y" or "F".

**Note:** The Natural RPC Session Parameters screen is displayed by pressing PF8 on the Session Parameters screen.

### **Additional Options/Restrictions/Session Parameters - RPC Restrictions/Logon Option**

This option determines which logon data are evaluated when the library is accessed by the RPC server. The following settings are available:

N	Library ID, user ID and password are evaluated.
A	Only library ID and user ID are evaluated (similar to the Natural profile parameter AUTO=ON, but for the current library only).

### **Command Restrictions**

The SCAN command is now verified.

### **Statement Restrictions**

The following Natural statements can now also be allowed/disallowed: CALLDBPROC, CLOSE CONVERSATION, CREATE OBJECT, DEFINE CLASS, DEFINE WORK FILE, END-RESULT, OPEN CONVERSATION, SEND METHOD.

## **Other Enhancements**

### **Return to Active Library**

A setup record is written for the first library the user logs on to (or for the default library when AUTO=ON). This setup record is used to establish a return library to which control is returned when a RETURN is issued. The library ID in the setup record is used to create the LOGON command. For further information, see the section SETUP in your Command Reference documentation.

### **Location of Source Modules Available with Natural Security**

The source modules for modules which are delivered with source code, such as user exits, logon exits, logon maps and interface sample programs, can now be found in the library SYSSEC. The maps for mailbox display, NSC-M--1 and NSC-M--2 have been replaced by the maps NSC-MY-1 and NSC-MY-2 respectively. If you wish to customize logon or user exits, refer to the appropriate sections of the Natural Security documentation for information on where to copy the object modules.

### **PROFILE Command - Special Link Indicated**

The Natural system command PROFILE shows the user the conditions of use currently in effect. The current value of the Natural system variable \*GROUP is shown in the Link ID field. Now an asterisk (\*) next to the ID indicates that the group's/user's link to the current library is a Special Link.

### **Interface Subprogram NSCXR**

The interface subprogram NSCXR provides the following three new functions:

- List cross references for command processors  
Lists all libraries and users for a command processor and lists the status of the functional security definition. For further information, see the example program PGMXR012.
- List available utility profiles  
For further information, see the example program PGMXR013.
- Retrieve user ID or library ID  
You specify the name of the user or library, and the interface subprogram will return the corresponding user/library ID. For further information, see example program PGMXR014.

Example programs `PGMXRnnn` showing how to invoke the subprogram `NSCXR`, as well as the explanatory texts `TXTXRnnn`, are provided in source form in the library `SYSSEC`.

### **Interface Subprogram NSCMA**

The subprogram `NSCMA` is used to perform maintenance/retrieval functions for mailbox security profiles from outside of the library `SYSSEC`.

Example programs `PGMXRnnn` showing how to invoke the subprogram `NSCMA`, as well as explanatory texts `TXTMAnnn`, are provided in source form in the library `SYSSEC`.